

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Peter Nesz, et al. § Group Art Unit: 2446
Application No 10/531,753 § § Examiner: Taha, Shaq
Filed: 09/20/2005 § § Confirmation No: 6062
§ §

Attorney Docket No: P17299-US1
Customer No.: 27045

For: Method and Arrangement for Preventing Illegitimate Use of IP Addresses

Via EFS-Web

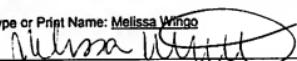
Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF TRANSMISSION BY EFS-WEB

Date of Transmission: September 30, 2009

I hereby certify that this paper or fee is being transmitted to the United States Patent and Trademark Office electronically via EFS-Web.

Type or Print Name: Melissa Wingo



APPEAL UNDER 35 U.S.C. §134

This Brief is submitted in connection with the decision of the Primary Examiner set forth in Final Office Action dated March 31, 2009, finally rejecting claims 13-22, which are all of the pending claims in this application, and the Advisory Action issued on June 30, 2009, maintaining the claim rejections set out in the Final Office Action.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §41.20(b)(2) that may be required by this paper, and to credit any overpayment, to Deposit Account No. 50-1379.

Real Party in Interest

The real party in interest, by assignment, is: Telefonaktiebolaget LM Ericsson (publ)
SE-164 83
Stockholm, Sweden

Related Appeals and Interferences

None.

Status of Claims

Claims 1-12 were previously cancelled and are not appealed. Claims 13-22 are pending in the present application, each of which are finally rejected and form the basis for this Appeal. Claims 13-16 and 18-21, stand rejected, under 35 U.S.C. §103(a), as being unpatentable over Sitaraman, *et al.* (U.S. Patent No. 6,427,170) in view of Alkhatib, *et al.* (U.S. Patent Publication No. 2004/0044778) and Lim, *et al.* (U.S. Patent No. 5884024); and claims 17 and 22 as being unpatentable over Sitaraman in view of Alkhatib and Taylor, *et al.* (U.S. Patent Publication No. 2002/0065919). Claims 13-22, including all amendments to the claims, are attached in the Claims Appendix. The rejection of claims 13-22 is appealed.

Status of Amendments

The claims set out in the Claims Appendix include all entered amendments. No amendment has been filed subsequent to the final rejection.

Summary of Claimed Subject Matter

Claim Element	Specification Reference
13. A method for preventing illegitimate use of an Internet Protocol (IP) address by a subscriber device in an IP network, the network including a switch node and at least one DHCP server, said subscriber device in communication with the switch node, the method including the steps of:	Page 5, line 33, <i>et seq.</i>
creating a list of trusted ones of the DHCP servers in said switch node;	Page 6, line 3, <i>et seq.</i>
transmitting by the subscriber device a DHCP request message for an IP address;	Page 6, line 9, <i>et seq.</i>
receiving a reply message by said switch node which carries an assigned subscriber IP address;	Page 6, line 11, <i>et seq.</i>
analysing the reply message by said switch node to be a DHCP message and having a source address from one of the trusted DHCP	Page 6, line 15, <i>et seq.</i>

servers;	
updating a filter dynamically in the switch node, the filter storing an identification of the subscriber device and the assigned subscriber IP address;	Page 6, line 21, <i>et seq.</i>
transmitting a frame from the subscriber device using a source IP address;	Page 6, line 26, <i>et seq.</i>
comparing in the filter said source IP address with the stored subscriber IP address; and,	Page 6, line 27, <i>et seq.</i>
discarding said frame when said source IP address differs from the stored subscriber IP address.	Page 6, line 31, <i>et seq.</i>

Claim Element	Specification Reference
18. A switch node in an Internet Protocol (IP) network adapted to prevent illegitimate use of an IP address by a subscriber device, the switch node including:	Page 5, line 5, <i>et seq.</i> Page 5, line 33, <i>et seq.</i>
at least one port for communication with a subscriber device;	Page 5, line 7, <i>et seq.</i>
an uplink port for communication with DHCP servers in the network; and,	Page 5, line 5
a filter device having a list of trusted ones of the DHCP servers, the filter device being associated with the ports; wherein the switch node is operative to:	Page 6, line 3, <i>et seq.</i>
receive a subscriber IP address request message from a subscriber device, analyse it to be a DHCP request message and transmit it on the uplink port;	Page 6, line 9, <i>et seq.</i>
receive a reply message on the uplink port, analyse it to be a DHCP reply message having a source IP address from one of the trusted DHCP servers on the list;	Page 6, line 11, <i>et seq.</i> Page 6, line 15, <i>et seq.</i>
dynamically update the filter with an identification of the subscriber device and a corresponding assigned subscriber IP address contained in the DHCP reply message;	Page 6, line 21, <i>et seq.</i>
receive a frame with a source IP address from a subscriber device;	Page 6, line 26, <i>et seq.</i>
compare in the filter said source IP address with the stored subscriber IP address for the subscriber device; and,	Page 6, line 27, <i>et seq.</i>
to discard said frame when said source	Page 6, line 31, <i>et seq.</i>

IP address differs from the stored subscriber IP address.

The specification references listed above are provided solely to comply with the USPTO's current regulations regarding appeal briefs. The use of such references should not be interpreted to limit the scope of the claims to such references, nor to limit the scope of the claimed invention in any manner.

Grounds of Rejection to be Reviewed on Appeal

- 1.) Claims 13-16 and 18-21 stand rejected, under 35 U.S.C. §103(a), as being unpatentable over Sitaraman, *et al.* (U.S. Patent No. 6,427,170) in view of Alkhatib, *et al.* (U.S. Patent Publication No. 2004/0044778) and Lim, *et al.* (U.S. Patent No. 5884024).
- 2.) Claims 17 and 22 stand rejected, under 35 U.S.C. § 103(a), as being unpatentable over Sitaraman in view of Alkhatib and Taylor, *et al.* (U.S. Patent Publication No. 2002/0065919).

Arguments

The Examiner rejected claims 13-16 and 18-21 as being unpatentable over Sitaraman, *et al.* (U.S. Patent No. 6,427,170) in view of Alkhatib, *et al.* (U.S. Patent Publication No. 2004/0044778) and Lim, *et al.* (U.S. Patent No. 5884024); and claims 17 and 22 as being unpatentable over Sitaraman in view of Alkhatib and Taylor, *et al.* (U.S. Patent Publication No. 2002/0065919). The Applicants traverse the rejections.

- 1.) **Claims 13-16 and 18-21 are patentable over Sitaraman, *et al.* (U.S. Patent No. 6,427,170) in view of Alkhatib, *et al.* (U.S. Patent Publication No. 2004/0044778) and Lim, *et al.* (U.S. Patent No. 5884024).**

In a non-final office action issued on October 23, 2008, the Examiner rejected claim 13-16 and 18-21 as being unpatentable over Sitaraman in view of Alkhatib. In the final office action issued on March 31, 2009, the Examiner merely added the teachings

of Lim to his stated basis of rejection of claims 13-16 and 18-21. For completeness herein, the Applicants will repeat their previously-submitted arguments which specifically distinguished claim 13 over the teachings of Sitaraman and Alkhatib, with added comments to point out where the Examiner has failed to address the points of those arguments and why the Examiner failed to establish how the teachings of Lim overcome the deficiencies identified by Applicants in the teachings of Sitaraman and Alkhatib.

The Applicants' invention is directed to preventing the illegitimate use of an Internet Protocol (IP) address in an IP network, commonly referred to as "spoofing." The novel method includes providing a filter in a switch node through which a subscriber device accesses the IP network. The switch node maintains a list of trusted DHCP servers which are conventionally used to assign an IP address to subscriber devices. When the switch node receives a DHCP request for an IP address from a subscriber device, the switch node examines the reply message that carries the assigned subscriber IP address and analyzes it to confirm it has a source address from one of the trusted DHCP servers. The switch node then dynamically updates the filter and stores an identification of the subscriber device and the assigned IP address. Subsequently, when the subscriber device transmits a frame using a source IP address, the switch node confirms in the filter that the source IP address of the frame matches the stored subscriber IP address and, if not, the switch node discards the frame. That combination of functions is not taught or suggested by the teachings of Sitaraman, Alkhatib and Lim, either individually or in combination.

With respect to the claim limitation "creating a list of trusted ones of the DHCP servers in said switch node," the Examiner refers generally to Sitaraman as disclosing, in Figure 2, "multiple DHCP servers." The Examiner, however, does not point to any teaching in Sitaraman, or Alkhatib, of creating a list of trusted ones of the DHCP servers, or storing such a list in the switch node through which a subscriber device accesses the IP network. Moreover, the Examiner has not pointed to any teaching in Lim of that claim limitation.

With respect to the claim limitation "analysing the reply message [by said switch node] to be a DHCP message and having a source address from one of the trusted DHCP

servers," the Examiner states that Sitaraman teaches a client that may decide to "accept [an offered IP address] or wait for additional offers from other DHCP servers on the network." That claim limitation now recites that the function is performed in the switch node and not the subscriber device (*i.e.*, the client). In either case, the Examiner does not point to any teaching in Sitaraman of analyzing a DHCP reply message to ensure that its source address is from a trusted one of the DHCP servers maintained in a list by the switch node. Similarly, if Sitaraman does not teach creating a filter list of trusted DHCP servers in a switch node, nor analyzing a reply message to be a DHCP message having a source address from one of the trusted DHCP servers, it cannot logically teach the claim limitation of "updating a filter dynamically in the switch node, the filter storing an identification of the subscriber device and the assigned subscriber IP address," which the Examiner asserts is taught at column 10, lines 27-31. The Applicants have examined the referenced portion of Sitaraman and find no such teaching. Moreover, the Examiner has not pointed to any teaching in Lim of that claim limitation.

With respect to the claim limitation "comparing in the filter said source IP address with the stored subscriber IP address," the Examiner states that Sitaraman teaches "dynamic" IP addresses are compared with static IP addresses," referring to column 4, lines 10-14. The claim limitation, however, read in the context of the whole claim, is comparing a source IP address of a frame from a subscriber device with a previously-stored IP address assigned to the subscriber device, in order to ensure the subscriber device is not "spoofing" an IP address not assigned to the device. Thus, the claim limitation is not comparing a dynamic IP address to a static IP address as the Examiner reads the teachings of Sitaraman. Moreover, the Examiner has not pointed to any teaching in Lim of that claim limitation.

The Examiner does recognize that Sitaraman fails to teach discarding a frame from a subscriber device when its source IP address differs from the stored subscriber IP address. The mere fact that the Examiner recognizes this deficiency in the teaching of Sitaraman should, as a logical matter, counter against his assertion that Sitaraman teaches the claim limitation of "comparing in the filter said source IP address with the stored subscriber IP address." The logical purpose of such comparison is to determine whether or not such addresses are the same and, thus, if they are not, the frame should

be discarded – the very function which the Examiner recognizes Sitaraman fails to teach. In either case, the Examiner looks to the teachings of Alkhatib to overcome the acknowledged deficiency. Alkhatib, however, fails to teach discarding, by a switch node, a frame transmitted by a subscriber device when the source IP address for the frame does not correspond to a previously-stored IP address assigned to the subscriber device. The Examiner points to paragraph 149 of Alkhatib as teaching this single limitation of claim 13. According to the teachings of Alkhatib, entities 14, 16 and 18 are devices such as “mobile and non-mobile computing devices,” which correspond to the “subscriber device” as used in claim 13, and those devices are connected to an IP network through a Network Address Translation (NAT) device 12. (see Figure 1). Alkhatib is directed to a system for accessing an entity inside a private network. According to the teachings of paragraph 149, “[i]f NAT 12 checks the source IP address in incoming packets, rejecting those in which the source IP address is different than the destination IP address for which the connection was established in the first place.” The purpose of that function in Alkhatib is to control access to the devices 14, 16 and 18 in the private network behind the NAT 12, not to ensure that source IP address utilized by such devices matches an IP address previously-assigned to such devices. Therefore, the Examiner’s reliance on the teachings of Alkhatib is inapposite and fails to cure the deficiencies in the teachings of Sitaraman. Moreover, the Examiner has not pointed to any teaching in Lim of that claim limitation.

Accordingly, the Examiner has not established a *prima facie* case of obviousness of claim 13 in view of Sitaraman, Alkhatib and Lim. Whereas independent claim 18 recites limitations analogous to those of claim 13, it is also not obvious over Sitaraman in view of Alkhatib. Furthermore, whereas claims 14-17 and 19-22 are dependent from claims 13 and 18, respectively, and include the limitations thereof, they are also not obvious in view of those references.

2.) Claims 17 and 22 are patentable over Sitaraman in view of Alkhatib and Taylor, et al. (U.S. Patent Publication No. 2002/0065919).

In a non-final office action issued on October 23, 2008, the Examiner rejected claims 17 and 22 as being unpatentable over Sitaraman in view of Alkhatib and Taylor. In the final office action issued on March 31, 2009, the Examiner did not modify the

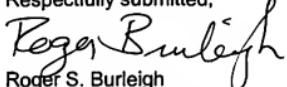
basis of rejection of claims 17 and 22, even though those claims are dependent from claims 13 and 18, respectively, which the Examiner rejected as unpatentable over Sitaraman in view of Alkhatib and Lim. In responding to the Final office action, the Applicants treated the Examiner's rejection of claims 17 and 22 as though they were rejected as being unpatentable over Sitaraman in view of Alkhatib, Lim and Taylor. As established *supra*, the Examiner has not established a *prima facie* case of obviousness of claims 13 and 18. Therefore, whereas claims 17 and 22 are dependent from those claims, and include the limitations thereof, they are not obvious over Sitaraman in view of Alkhatib, Lim and Taylor.

* * *

CONCLUSION

Claims 13-22 are patentable over the teachings of Sitaraman in view of Alkhatib, Lim and Taylor and, therefore, the Applicants request that the Examiner's rejection thereof be reversed and the application be remanded for further prosecution.

Respectfully submitted,


Roger S. Burleigh
Registration No. 40,542
Ericsson Patent Counsel

Date: September 30, 2009

Ericsson Inc.
6300 Legacy Drive, M/S EVR1 C-11
Plano, Texas 75024

(972) 583-5799
roger.burleigh@ericsson.com

CLAIMS APPENDIX

1-12. (Cancelled)

13. (Previously Presented) A method for preventing illegitimate use of an Internet Protocol (IP) address by a subscriber device in an IP network, the network including a switch node and at least one DHCP server, said subscriber device in communication with the switch node, the method including the steps of:

- creating a list of trusted ones of the DHCP servers in said switch node;
- transmitting by the subscriber device a DHCP request message for an IP address;
- receiving a reply message by said switch node which carries an assigned subscriber IP address;
- analysing the reply message by said switch node to be a DHCP message and having a source address from one of the trusted DHCP servers;
- updating a filter dynamically in the switch node, the filter storing an identification of the subscriber device and the assigned subscriber IP address;
- transmitting a frame from the subscriber device using a source IP address;
- comparing in the filter said source IP address with the stored subscriber IP address; and,
- discarding said frame when said source IP address differs from the stored subscriber IP address.

14. (Previously Presented) The method according to claim 13, further comprising the step of storing in the filter a subscriber MAC address, a subscriber physical port number, a subscriber virtual LAN identity and a lease time interval for the assigned subscriber IP address.

15. (Previously Presented) The method according to claim 13, wherein the subscriber IP address is statically assigned and handled by the DHCP servers.

16. (Previously Presented) The method according to claim 14, the method including deleting the subscriber identification and the corresponding assigned subscriber IP address from the filter when the lease time interval is out.

17. (Previously Presented) The method according to claim 13, the method further comprising the steps of:

counting a number of attempts (n) from the subscriber to use an illegitimate IP address;

comparing the number (n) of the attempts with a threshold number (N);

sending a warning signal when the number of attempts exceeds a threshold criteria.

18. (Previously Presented) A switch node in an Internet Protocol (IP) network adapted to prevent illegitimate use of an IP address by a subscriber device, the switch node including:

at least one port for communication with a subscriber device;

an uplink port for communication with DHCP servers in the network; and,

a filter device having a list of trusted ones of the DHCP servers, the filter device being associated with the ports; wherein the switch node is operative to:

receive a subscriber IP address request message from a subscriber device, analyse it to be a DHCP request message and transmit it on the uplink port;

receive a reply message on the uplink port, analyse it to be a DHCP reply message having a source IP address from one of the trusted DHCP servers on the list;

dynamically update the filter with an identification of the subscriber device and a corresponding assigned subscriber IP address contained in the DHCP reply message;

receive a frame with a source IP address from a subscriber device;

compare in the filter said source IP address with the stored subscriber IP address for the subscriber device; and,

to discard said frame when said source IP address differs from the stored subscriber IP address.

19. (Previously Presented) The switch node according to claim 18, wherein the switch node is further operative to store in the filter a subscriber MAC address, a subscriber physical port number, a subscriber virtual LAN identity and a lease time interval for the assigned subscriber IP address.

20. (Previously Presented) The switch node according to claim 18, wherein the subscriber IP address comprises a statically assigned address which is handled by the DHCP servers.

21. (Previously Presented) The switch node according to claim 19, wherein the switch node is further operative to delete the subscriber identification and the corresponding assigned subscriber IP address from the filter when the lease time interval expires.

22. (Previously Presented) The switch node according to claim 18, wherein the filter comprises a counter operative to count a number (n) of discarded frames on the subscriber port, to compare the number (n) of the discarded frames with a threshold number (N), and to send a warning signal when the number of discarded frames exceeds a threshold criterion.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.